What is claimed is:

1. A content decryption device that decrypts encrypted content that is recorded on a recording medium, and outputs the decrypted content to an external device, comprising:

decryption means for decrypting the encrypted content to generate the decrypted content; and

instruction execution means for decoding a transfer instruction that includes a transfer destination address showing a position of a content output means in an address space as a transfer destination of the decrypted content to extract the transfer destination address, and outputting the extracted transfer destination address to an address detection means;

the address detection means for pre-storing a permitted address that shows a transfer destination to which output of the decrypted content is permitted, judging whether the transfer destination address matches the permitted address, and outputting, only when the transfer destination address matches the permitted address, the decrypted content to the content output means whose position is shown by the transfer destination address; and

the content output means for receiving the decrypted content, and outputting the received decrypted content to the external device.

2. The decryption device of Claim 1 further comprising:

obtaining means for obtaining, from another external device, a decryption program including (a) a decryption instruction that shows decryption of encrypted content, and (b) a transfer instruction that includes the transfer destination address showing the position in the content output means, and that shows transfer of the decrypted content to the content output means,

wherein the decryption means decrypts the encrypted content according to the decryption instruction, and

the instruction execution means outputs the transfer destination address according to the transfer instruction.

3. The content decryption device of Claim 2,

wherein the decryption means, the instruction execution means, the address detection means, the content output means and the obtaining means are connected via a bus,

the instruction execution means outputs the transfer destination address via the bus,

the address detection means obtains the transfer destination address via the bus, and outputs the decrypted content via the bus, and

the content output means receives the decrypted content

via the bus.

4. The content decryption device of Claim 3,

wherein the address detection means further has a state in which the permitted address is not stored, and

the content decryption device further comprises:

state control means for judging whether the address detection means stores the permitted address, and, when the address detection means is judged not to store the permitted address, prohibiting the instruction execution means from executing the transfer instruction.

5. The content decryption device of Claim 3,

wherein the obtaining means further obtains, from the other external device, an encrypted permitted address that is a new permitted address which has been encrypted,

the decryption means decrypts the encrypted permitted address to generate the new permitted address,

the address detection means stores the generated new permitted address in place of the permitted address, and when encrypted content is next decrypted, judges whether the transfer destination address and the new permitted address match.

6. The content decryption device of Claim 5,

wherein the decryption means pre-stores a variable key, and decrypts the encrypted permitted address using the variable key.

7. The content decryption device of Claim 6,

wherein the decryption means further pre-stores a unique key that is unique to the content decryption device,

the obtaining means further obtains an encrypted variable key that is a new variable key that has been encrypted using the unique key,

the decryption means decrypts the encrypted variable key using the unique key to generate the new variable key, and stores the generated new variable key in place of the variable key, and uses the new variable key when next decrypting a permitted address that has been encrypted using the new variable key.

8. The content decryption device of Claim 6,

wherein the decryption means further has a state in which the variable key is not stored, and

the state control means further judges whether the decryption means stores the variable key, and, when the decryption means is judged not to store the variable key, prohibits the decryption means from decrypting.

9. The content decryption device of Claim 1,

wherein the decryption means, the instruction execution means and the address detection means together compose a CPU,

a first authentication is performed between the CPU and the recording medium, and following the first authentication a second authentication is performed between the CPU and the content output unit, and

the content decryption device decrypts the encrypted content and outputs the decrypted content to the external device only when both the first authentication and the second authentication are successful.

10. A content decryption device that decrypts encrypted content and outputs the decrypted content to an external device, comprising:

obtaining means for obtaining, from another external device, a decryption program that includes a program for decrypting encrypted content and outputting the decrypted content to the external device, and that includes first encrypted information and second encrypted information, the first encrypted information having been generated by encrypting a predetermined piece of information according to a first encryption, the second encrypted information having been

generated by encrypting the predetermined piece of information according to a second encryption;

storage means for storing the program;

decryption means for decrypting the first encrypted information according to a first decryption to generate first decrypted information, and decrypting the second encrypted information according to a second decryption to generate second decrypted information, the first decryption being an inverse transformation of the first encryption, and the second decryption being an inverse transformation of the second encryption; and

judgement means for judging whether the first decrypted information and the second decrypted information match, and when the first decrypted information and the second decrypted information are judged not to match, prohibiting execution of the program.

11. The content decryption device of Claim 10,

wherein the first encryption is encryption in which a predetermined encryption algorithm is applied using a first key,

the second encryption is encryption in which the predetermined encryption algorithm is applied using a second key,

the first decryption is decryption in which a predetermined decryption algorithm is applied using a first key, the predetermined decryption algorithm being an inverse transformation of the predetermined encryption algorithm, and

the second decryption is decryption in which the predetermined decryption algorithm is applied using a second key.

12. The content decryption device of Claim 10,

wherein the first encryption is encryption in which a first encryption algorithm is applied using an encryption key,

the second encryption is encryption in which a second encryption algorithm is performed using the encryption key,

the first decryption is decryption in which a first decryption algorithm is performed using the encryption key, the first decryption algorithm being an inverse conversion of the first encryption algorithm, and

the second decryption is decryption in which the second decryption algorithm is performed using the encryption key, the second decryption algorithm being an inverse conversion of the second encryption algorithm.

13. The content decryption device of Claim 10, further comprising:

control means for executing initialization of the content decryption device when the judgement means judges that the first decrypted information and the second decrypted information do not match.

14. The content decryption device of Claim 10,

wherein the control means further, when the first decrypted information and the second decrypted information are judged not to match, requests the user to have the program stored in the storage means.

15. The content decryption device of Claim 14,

wherein the control means further judges whether the program has been updated, and, when the program is judged not to have been updated, prohibits execution of the program.

16. A content decryption device that decrypts encrypted content and outputs the decrypted content to an external device, comprising:

data storage unit for storing (a) a first encrypted key that has been generated by encrypting a common key using a CPU unique key that is unique to a CPU, and (b) a second encrypted key that has been generated by encrypting a common key using a content processing unit unique key that is unique to a content

processing unit;

the CPU for performing execution of instructions, encryption of information, and decryption of information, and for generating a common key by decrypting the first encrypted key using the CPU unique key, and storing the generated common key,

the content processing unit for (a) storing content, or outputting stored content to the external device, and (b) generating a common key by decrypting the second encrypted key using the content processing unit unique key.

17. The content decryption device of Claim 16,

wherein the CPU includes:

a key generation sub-unit for generating a new common key;

an encryption sub-unit for encrypting the new common key using the common key to generate an encrypted common key;

an output sub-unit for outputting the generated encrypted common key to the content processing unit; and

a key updating sub-unit for storing the new common key in place of the common key; and

the content processing unit includes:

an obtaining sub-unit for obtaining an encrypted common key;

a decryption sub-unit for decrypting the obtained

encrypted common key using the common key to generate a new common key; and

a key updating sub-unit for storing the new common key in place of the common key.

18. The content decryption device of Claim 16,

wherein the CPU includes:

an information storage sub-unit for storing predetermined information;

an encryption unit for encrypting the predetermined information using the common key to generate encrypted information;

an output sub-unit for outputting the generated encrypted information to the content processing unit; and

a key calculation sub-unit for applying a predetermined calculation to the common key and the predetermined information to generate a new common key, and storing the generated new common key in place of the common key, and

the content processing unit further includes:

an obtaining sub-unit for obtaining encrypted information;

a decryption sub-unit for decrypting the obtained encrypted information using the common key to generate a new common key; and

a key calculation sub-unit for applying a predetermined calculation that is the same as the predetermined calculation to the common key and the predetermined information to generate a new common key, and storing the generated new common key in place of the common key.